FortiAuthenticator™ 3.0

Release Notes

FortiAuthenticator™ 3.0 Release Notes

October 22, 2013

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions, resolved issues and known issues for FortiAuthenticator™ 3.0.

FortiAuthenticator is a User and Identity Management solution enabling including Strong Authentication, Wireless 802.1X Authentication, Certificate Management and Fortinet Single Sign-On.

For additional documentation, please visit:

http://docs.fortinet.com/fauth.html

Supported models

The following models are supported by FortiAuthenticator v3.0.

FortiAuthenticator 200D

FortiAuthenticator 400C

FortiAuthenticator 1000C

FortiAuthenticator 3000B

FortiAuthenticator 3000D

FortiAuthenticator VM

See http://docs.fortinet.com/fauth.html for additional documentation on FortiAuthenticator v3.0

Special Notices

TFTP boot process

The TFTP boot process erases all current FortiAuthenticator configuration and replaces it with the factory default settings.

Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the Web-based Manager to be viewed properly without need for scrolling.

Before any upgrade

Save a copy of your FortiAuthenticator unit configuration prior to upgrading. *Go to System* > *Maintenance* > *Config* and select *Download Backup File* to backup the configuration.

After any upgrade

If you are using the Web-based Manager, clear your browser cache prior to login on the FortiAuthenticator to ensure the Web-based Manager screens are displayed properly

Downgrading

If downgrading FortiAuthenticator from 3.0 to a prior release, due to a change in the Session Cookie format, login will fail. Before attempting to login following downgrade, clearing the browser cache will avoid this issue.

What's new

Before upgrading, review the following changes for impact to your unique deployment. Note that this list is not exhaustive but highlights the major feature enhancements in this release.

Windows Authentication for Microsoft Windows

Windows Authentication for Microsoft Windows is a plugin for Windows PCs which enables two factor authentication to be included during the Windows login process. This client is included free of charge with FortiAuthenticator™ 3.0 and can be downloaded from the GUI.

For installation and integration details see the Windows Authentication for Microsoft Windows Install Guide:

http://docs.fortinet.com/fauth.html

Guest portal enhancements

Several changes have been made to the guest portal to allow customization of the content displayed and the information collected during the registration process.

User device certificate self-enrolment

Extension to the user login portal to enable self-enrolment of certificates onto "Bring Your Own" devices using SCEP and other methods.

Fortinet Single Sign-On (FSSO) enhancements

Multiple new FSSO features added in FortiAuthenticator 3.0 including

- Hierarchical tiering of suppliers and collectors enabling scaling of FortiAuthenticator deployments
- Support collection of events from DC Agents FSSO software for Windows AD
- Support collection of events from TS Agents FSSO software for Citrix Servers
- FSSO Workstation logoff detection via WMI
- Ability to limit the number of concurrent devices a user can have authenticated

Scheduled configuration backup

Scheduled backup of configuration to remote server via FTP/SFTP

Extended API

API extended to support:

- Provisioning of new users and groups
- Authentication (and de-authentication) of users in FSSO

Upgrade instructions

Back up your configuration before beginning this procedure. Whilst no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Upgrading from previous releases - Hardware only

FortiAuthenticator hardware supports upgrade from FortiAuthenticator 2.0 MR2 and subsequent patch releases. Follow the standard Firmware Upgrade Process described below.

Upgrading from previous releases - VM only

Do not upgrade FortiAuthenticator virtual machine appliances directly from v.2.0 MR2 and lower to v.3.0. **This will result in data loss.** Please follow the procedure below.

Due to the default firmware partition size being too small to accommodate the expanded firmware, FortiAuthenticator-VM does not support upgrade from FortiAuthenticator 2.0 MR2 directly to FortiAuthenticator 3.0. To enable upgrade from FortiAuthenticator 2.0 MR2 (including PR1 and PR2), an interim upgrade step via FortiAuthenticator 2.0 MR3 is required. FortiAuthenticator 2.0 MR3 contains no functional feature enhancements but has been created to increase the firmware partition size prior to upgrading to FortiAuthenticator 3.0.

To upgrade, use the Firmware Upgrade Process below to upgrade initially to FortiAuthenticator 2.0 MR3 (build 210), then repeat the process to upgrade to FortiAuthenticator 3.0 ensuring to backup the firmware at each step.

Firmware upgrade process

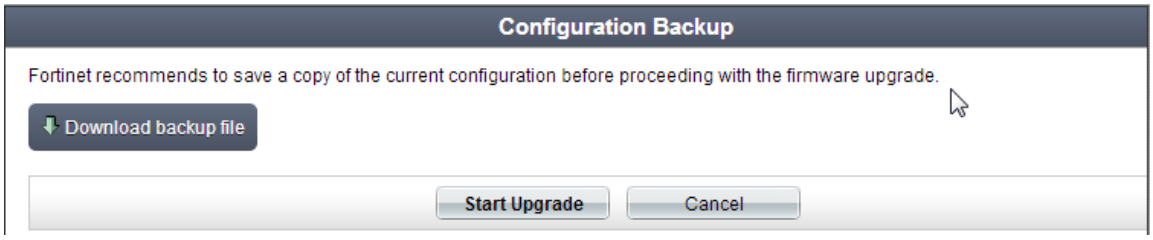
After backing up your configuration first, follow the following procedure to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware package from the Customer Service & Support web site, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Customer Service & Support web site at https://support.fortinet.com. In the Download section of the page, select the Firmware Images link to download the firmware.
2. To verify the integrity of the download, go back to the Download section of the login page, then click the *Firmware Image Checksums* link.
3. Log in to the FortiAuthenticator unit's Web-based Manager using the *admin* administrator account.
4. Go to *System* > *Dashboard* > *Status*.
5. In the *System Information* widget, in the *Firmware Version* row, select *Upgrade*. The *Firmware Upgrade* or *Downgrade* dialog box opens.

6. In the *Firmware* section, select *Choose File*, and locate the upgrade package that you downloaded.
7. Select *OK* to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



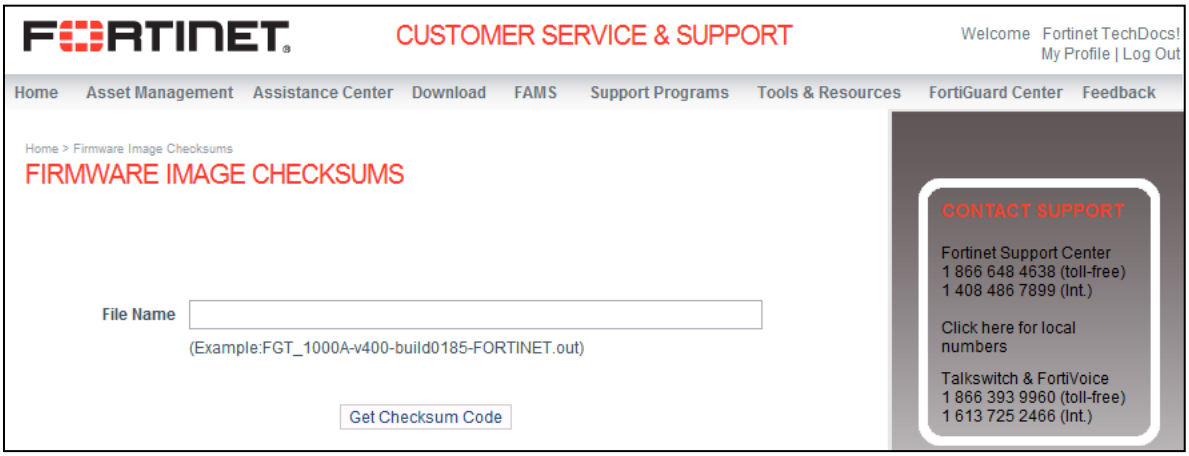
It is recommended that a system backup is taken at this point. Once complete, click ***Start Upgrade.***

Wait until the unpacking, upgrade and reboot process completes (usually 3-5 minutes), then refresh the page.

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, go to *Download* > *Firmware Image Checksums*. In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.



Product Integration and Support

Web browser support

The following web browsers are supported by FortiAuthenticator v2.0 MR2:

- Microsoft Internet Explorer versions 8 to 10
- Mozilla Firefox versions 15 to 17
- Google Chrome versions 22 to 30

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator v3.0 supports the following FortiOS versions:

- FortiOS v4.0 MR3 Patch Release 15
- FortiOS v5.0 Patch Release 4

Other FortiOS versions may function correctly, but are not supported by Fortinet.

Fortinet agent support

FortiAuthenticator v3.0 supports the following Fortinet Agent

- FortiClient v.5.0.5 for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 1.0.0
- FSSO DC Agent v.4.3.0142
- FSSO TS Agent v.4.3.0142

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which Operating Systems are supported by each Agent, please see the Install Guides provided with the software.

Virtualization software support

FortiAuthenticator v3.0 supports VMware ESXi / ESX 4.0, 4.1, 5.0 and 5.1.

See Appendix A: FortiAuthenticator VM for more information.

Third party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS). For more information, see the FortiAuthenticator Two-Factor Authentication Interoperability Guide http://docs.fortinet.com/fauth.html

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
162592	Machine names not resolved to IP in FSSO
184313	2FA cannot be deselected from remote user
184939	Remove redundant radius attributes
195486	Timeouts when provisioning more than 50 FortiToken Mobile tokens
196438	Reduce default FSSO logging level
197627	Download MIB link in SNMP GUI
199219	Remove need for webserver restart on HW license import
201062	GUI: Dashboard widget refresh prevents idle timeouts
203986	Accounting proxy initialization failed if rule added with same attributes
204853	FTM Timeout Setting
204877	LDAP import user page "Configure user attributes" fails
205128	Apply User password maximum length in GUI
205403	Radius Accounting - Source Password
206326	Token code displayed in cleartext
206327	Remote user is case sensitive if login portal set to use selected groups only
206469	Delay start of FSSO process until FortiAuthenticator is fully booted and HA negotiation complete
206489	FTM HA issue
206763	FSSO - Refresh logged-in users group membership periodically
206769	802.1x PEAP dynamic VLAN assignment via RADIUS does not work
207015	No GUI access after applying wildcard certificate.
207584	fac_ldap search goes into infinite loop consuming 100% CPU
207924	Local user creation confirm specified password
207973	FAC cannot identify utf-8 messages return from SMS-Gateway
207978	User self-registration fails if administrator approval not required
208733	Mobile number truncated on form save
209309	Support wildcard re-enrolment request

210051	Change log auditor doesn't log the user's username
210189	Intermediary CA Creation requires private key for import
210796	Possible to add local user to remote LDAP group
212150	GUI: Device certificate expiry notification failed
212368	FAC does not strip realm from username for LDAP search.
212471	User registration - field configuration
212541	No gratuitous ARP send on HA failover
214215	FTM trial tokens not possible for licensed VM
214436	NAS Client user authentication, username is case sensitivity inconsistency
214750	Domain Controller Admin account format
214999	ARP Flux Issue
213149 215263	SSO portal logout doesn't send accounting stop request
217202	Maintainer account doesn't work on VM
172050	GUI: Various extra logging for LDAP browser/import
182328	GUI: 2nd admin dashboard on HA slave shows an error
187623	Authentication logs for web service is under a wrong category
188747	Invalid IP address format is accepted for Auth Client
192371	GUI: Warn Admin when referenced certificate is revoked or expired
196211	GUI: form error when enabling email recovery with only an alternative email set
196213	GUI: recover by email throws error if more than one users has the same primary email
196214	Implement user lock out for security question
197038	System resource widget settings crash
197988	Allow longer DN for Domain Controller account
199365	GUI: Invalid IP address format is accepted
200778	GUI: Failed login attempt to the user portal site is not shown in the Auth Activity chart
200783	Log if remote admin backup password is being used
202979	User DN - tool tip
203018	GUI: Invalid entries (non-integer) accepted in SNMP integer fields
204565	GUI: IE bug - Security question shown as disabled
208547	Include more files in report.dbg
211434	Add static route with heartbeat interface as network interface
212411	VM license not taken into account if HA parameters are configured
212553	B0208: SSO portal with LDAP authentication only work if LDAP is reachable

	through port1
212554	SSO groups import only work if LDAP is reachable through port1
212923	[FG-IR-13-016] removal of root shell
212961	FGT 2-step auth allow token code with extra ending characters
158664	GUI: Configurable site name
163986	GUI: Remote LDAP search can't handle non-ascii character
198952	New Fortinet RADIUS VSAs
202173	Duplicate Computer name existing on domain does not give descriptive error
202522	GUI: Certificate creation subject fields in wrong order
204752	GUI: Recommend config backup before upgrade
206992	High CPU triggered by radacctd process
207403	SSO Excluded user import needs to filter out computers/groups
208099	MemberOf failure due to ";first entry NULL"; when using FAC's local LDAP
209773	B0208: User registration receipt message incorrect hyperlinks
210902	GUI: Remote LDAP username should be case-insensitive
211826	Add infoblox in radius dictionaries
212555	Windows AD IP address includes TCP port in monitor page

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
206462	TELNET reverse DNS lookup causes unnecessary login delay
213022	Oversized images can obscure display in Image Upload utility
215227	Remote user sync does not import all users in some cases
216032	GUI - Mass user import can fail with timeout (includes manual remote user sync)

Appendix A: FortiAuthenticator VM

FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator VM system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported virtual machine (VM) environment. For details, see the Install Guide for FortiAuthenticator VM available at http://docs.fortinet.com.

Table 3: VM Requirements

Virtual Machine	Requirement
Hypervisor Support	VMware ESXi / ESX 4.0, 4.1, 5.0 and 5.1
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Virtual CPUs Supported (Minimum / Maximum)	1 / 8
Virtual NICs Supported (Minimum / Maximum)	1 / 4
Storage Support (Minimum / Maximum)	60GB / 2TB
Memory Support (Minimum / Maximum)	512 MB / 4GB
High Availability Support	Yes

FortiAuthenticator VM firmware

Fortinet provides FortiAuthenticator VM firmware images in two formats:

- ***.out:*** Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- ***ovf.zip***: Use this image for new VM installations. It contains a deployable Open Virtualization Format (OVF) virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortiauthenticator/index.html

Appendix B: Maximum values

This section lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware and VM configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Hardware appliances

The following table describes the maximum values set for the various hardware models.

Table 4: Maximum values - Hardware.

Feature		Model				
		FortiAuthenticator 200D	FortiAuthenticator 400C	FortiAuthenticator 1000C	FortiAuthenticator 3000B	FortiAuthenticator 3000D
System						
Network	Static Routes	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20
	SMS Gateways	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20
Administration	SYSLOG Servers	20	20	20	20	20
	User Uploaded Images	25	100	500	1000	2000
	Language Files	50	50	50	50	50
Authentication						
General	Auth Clients (NAS)	50	200	1000	2000	4000
Local User Management	**Users** (Local + Remote)[1]	500	2000	10000	20000	40000
	User Radius Attributes	1500	6000	30000	60000	120000

	User Groups	50	200	1000	2000	4000
	Group Radius Attributes	150	150	600	6000	120000
	FortiTokens	1000	4000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200
	LDAP Entries	1000	4000	20000	40000	80000
	Device (MAC-based Auth.)	50	200	1000	2000	4000
	Remote LDAP Servers	20	80	400	800	1600
	Remote LDAP Sync Rule	25	100	500	1000	2000
	Remote LDAP User Radius Attributes	1500	6000	30000	60000	120K
SSO & Dynamic Policies						
SSO	SSO Users	500	2000	10000	20000	200K [3]
	SSO Groups	1000	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	4000
	RADIUS Accounting SSO Clients	50	200	1000	2000	4000
	FortiGate Services	50	200	1000	2000	4000
	FortiGate Group Filtering	250	1000	5000	10000	20000
	FSSO Tier Nodes	5	20	100	200	400
	IP Filtering Rules	250	1000	5000	10000	20000
Accounting Proxy	Sources	50	200	1000	2000	4000
	Destinations	25	100	500	1000	2000
	Rulesets	25	100	500	1000	2000
Certificates						
User Certificates	User Certificates	2500	10000	50000	100K	200K
	Server Certificates	50	200	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50
	Trusted CA Certificates	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200
SCEP	Enrollment Requests	500	2000	10000	20000	40000

[1] Note that there is one metric used for the number of allowed users which is *Users*. Local Users and Remote Users share the same limit value. This enables Local Users ***or*** Remote Users to be equal to *Users* or for there to be a mixture of user types, however, the total number of Local and Remote Users cannot exceed *the Users* metric.

[2] *FortiToken Mobile Licenses* refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000D, the total number of concurrent SSO Users is set to a higher level to cater for large deployments.

VM appliances

The FortiAuthenticator-VM Appliance is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator VM-Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The Calculating Metric column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator-VM Base License, the number of Auth Clients (NAS Devices) that can authenticate to the system is:

$$100 \Big/ 10 = 10$$

Where this relative system is not used e.g. for static routes, the *calculating metric* is denoted by a '-'. The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Table 5: Maximum Values - Virtual Machines.

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	SYSLOG Servers	2	20	20	20
	User Uploaded Images	5	Users / 20	5	100
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 10	10	500
User Management	**Users** (Local + Remote)*	5	**********	100	5000
	User Radius Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500

	Group Radius Attributes	9	User x 3	300	15000
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked)	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	1	Users / 10	10	500
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Sync Rule	1	Users / 20	5	250
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
SSO & Dynamic Policies					
SSO	SSO Users	5	Users	100	5000
	SSO Groups	30	Users / 2	50	2500
	Domain Controllers	3	Users / 10	10	50
	RADIUS Accounting SSO Clients	3	Users / 10 (min=10)	10	50
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users /100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
Accounting Proxy	Sources	3	Users / 10	10	500
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	200	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users	100	5000

[1] Note that there is one metric used for the number of allowed users which is *Users*. Local Users and Remote Users share the same limit value. This enables Local Users ***or*** Remote Users to be equal to *Users* or for there to be a mixture of user types, however, the total number of Local and Remote Users cannot exceed *the Users* metric.

[2] *FortiToken Mobile Licenses* refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] Minimum value overrides Calculating Metric in this case